JORDAN L. LURIE, State Bar No. 130013
ARI Y. BASSER, State Bar No. 272618
POMERANTZ LLP
1100 Glendon Avenue, 15th Floor
Los Angeles, CA 90024
Telephone: (310) 432-8492
jllurie@pomlaw.com
abasser@pomlaw.com

STEPHEN R. BASSER, State Bar No. 121590
SAMUEL M. WARD, State Bar No. 216562
BARRACK RODOS & BACINE
One America Plaza
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874
sbasser@barrack.com
sward@barrack.com

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

MARCOS RAMOS, RIGOBERTO RAMOS, and ARGERE FRUDAKIS, on behalf of themselves and all others similarly situated,

Plaintiffs

v.

REGAL MEDICAL GROUP, INC.,

Defendant

Civil Action No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Marcos Ramos ("M. Ramos"), Rigoberto Ramos ("R. Ramos") and Argere Frudakis ("Frudakis") (collectively "Plaintiffs"), by and through their attorneys of record, upon personal knowledge as to their own acts and experiences, and upon information and belief as to all other matters, bring this class action complaint against Regal Medical Group, Inc., and allege as follows:

INTRODUCTION

1. Plaintiffs bring this class action against Defendant Regal Medical Group, Inc., ("Defendant" or "Regal") for its failure to properly secure and safeguard Plaintiffs' and Class Members' protected health information and personally identifiable information stored within Defendant's information network and servers, including, without limitation, medical information such as information regarding medical treatments, provider names, dates of service, diagnosis/procedure information, (these types of information, *inter alia*, being hereafter referred to, collectively, as "protected health information" or "PHI"),[1] account numbers and/or record numbers, names, and dates of birth (these latter types of information, *inter alia*, being hereafter referred to, collectively, as "personally identifiable information" or "PII").[2]

2. Plaintiffs seek to hold Defendant responsible for the harms it caused and will continue to cause Plaintiffs and over 3 million others similarly situated persons by virtue of a massive and preventable cyberattack that began no later than December 1, 2022, and was

[1] Protected Health Information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. Inter alia, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories, and data points applied to a set of demographic information for a particular patient. PHI is inclusive of and incorporates personally identifiable information.

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

discovered by Defendant on December 2, 2022, if not sooner, by which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed highly sensitive PII and PHI and financial information which was being kept unprotected (the "Data Breach"). Plaintiffs further seek to hold Defendant responsible for not ensuring that the PII and PHI was maintained in a manner consistent with industry standards, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule (45 CFR, Parts 160 and 164(A) and (E)), the HIPAA Security Rule (45 CFR, Parts 160 and 164(A) and (C)), and other relevant standards.

3. While Defendant claims to have discovered the Data Breach as early as December 2, 2022 (although the right is reserved to produce evidence that it occurred and was discovered even sooner), it delayed informing victims of the Data Breach commencing no earlier than February 1, 2023 and thereafter. Indeed, Plaintiffs and Class Members were wholly unaware of the Data Breach until they received notification letters from Defendant informing them of it (the "Notice"), commencing on or about February 1-2, 2023 and at various times thereafter.

4. Defendant acquired, collected, and stored Plaintiffs' and Class Members' PII and PHI and/or financial information to facilitate the healthcare services Plaintiffs and Class Members requested or received. Defendant knew, at all times material, that networks stored sensitive data, including Plaintiffs' and Class Members' highly confidential PII and PHI.

5. HIPAA establishes obligations for the protection of individuals' medical records and other personal health information. HIPAA, in general, applies to healthcare providers, health plans/insurers, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically, and sets requirements for Defendant's maintenance of Plaintiffs' and Class Members' PII and PHI. More specifically, HIPAA requires appropriate safeguards be maintained by organizations such as Defendant to protect the privacy of patient health information and sets limits and conditions on the uses and disclosures that may be made of such information without express customer/patient authorization. HIPAA also gives a series of rights to patients over their PII

and PHI, including rights to examine and obtain copies of their health records, and to request corrections thereto.

6. Additionally, the so-called ”HIPAA Security Rule” establishes national standards to protect individuals’ electronic health information that is created, received, used, or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI.

7. By obtaining, collecting, using, and deriving a benefit from Plaintiffs’ and Class Members’ PII and PHI, Defendant assumed legal and equitable duties to those individuals. These duties arise from HIPAA and other state and federal statutes and regulations, as well as common law principles. HIPAA provides the standard of procedure by which a medical provider must operate when collecting, storing, and maintaining PHI and imposes a duty on Regal to maintain the confidentiality of such information. Defendant is charged, *inter alia*, with legal violations predicated upon the duties set forth in HIPAA that underpin those violations and that were not honored, or were otherwise breached by Regal.

8. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs’ and Class Members’ PII and PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII and PHI of Plaintiffs and Class Members were compromised and damaged through access by and disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiffs and Class Members in the future – and are entitled to damages. In addition, Plaintiffs and Class Members, who have a continuing interest in ensuring that their information is and remains safe, are entitled to injunctive and other equitable relief.

PARTIES

Plaintiff Marcos Ramos

9. Plaintiff Marcos Ramos ("M. Ramos") is, and at all times material hereto has been, a resident and citizen of San Fernando, California. Plaintiff M. Ramos received a letter entitled "Notice of Data Breach" dated February 6, 2023, which notified Plaintiff Ramos that "on Friday, December 2, 2022, [Defendant] noticed difficulty in accessing some of our servers … malware was detected on some of our servers, which … resulted in the threat actor accessing and infiltrating certain data from our systems …." ("Notice Letter").

10. The Notice Letter further informed Plaintiff M. Ramos that his PHI and PII may have been impacted including his name, social security number, date of birth, address, diagnosis and treatment, laboratory test results, prescription data, radiology reports, health plan member number, and phone number.

11. Upon information and belief, Defendant continues to maintain Plaintiff M. Ramos' PHI and PII, as well as that of all other Class Members.

Plaintiff Rigoberto Ramos

12. Plaintiff Rigoberto Ramos ("R. Ramos") is, and at all times material hereto has been, a resident and citizen of San Fernando, California. Plaintiff R. Ramos received a letter entitled "Notice of Data Breach" dated February 6, 2023, which notified him that "on Friday, December 2, 2022, [Defendant] noticed difficulty in excessing some of our servers … malware was detected on some of our servers, which … resulted in the threat actor accessing and infiltrating certain data from our systems …."

13. The Notice Letter further informed Plaintiff R. Ramos that his PII and PHI may have been impacted including his name, social security number, date of birth, address, diagnosis and treatment, laboratory test results, prescription data, radiology reports, health plan member number, and phone number.

14. Upon information and belief, Defendant continues to maintain Plaintiff R. Ramos' PHI and PII, as well as that of all other Class Members.

Plaintiff Argere Frudakis

15. Plaintiff Argere Frudakis, ("Frudakis") and at all times material hereto has been, a resident and citizen of Laguna Hills, California. Plaintiff Frudakis received a letter entitled "Notice of Data Breach" dated February 1, 2023, which notified him that "on Friday, December 2, 2022, [Defendant] noticed difficulty in excessing some of our servers … Malware was detected on some of our servers, which … resulted in the threat actor accessing and infiltrating certain data from our systems …." ("Notice Letter").

16. The Notice Letter further informed Plaintiff Frudakis that his PII and PHI may have been impacted including his name, social security number, date of birth, address, diagnosis and treatment, laboratory test results, prescription data, radiology reports, health plan member number, and phone number.

17. Upon information and belief, Defendant continues to maintain Plaintiff Frudakis' PHI and PII, as well as that of all other Class Members.

Defendant Regal Medical Group, Inc.

18. Defendant Regal Medical Group, Inc., ("RMG") a healthcare network providing medical services, maintains its principle office at 8510 Balboa Boulevard, Suite 275, Northridge, California. Defendant RMG acquired, utilized and stored the PHI/PII of Plaintiffs named herein and Class Members respecting whom Plaintiffs seek to represent.

19. RMG, founded in September 1994, is one of the largest physician-led healthcare networks in Southern California, with over 3000 primary care doctors, 10,000 specialists, hundreds of hospitals, urgent care centers, and labs for patients, and more than 500,000 members. It is an affiliated medical group" of Heritage Provider Network, Inc., based in California.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, which affords federal courts with original

jurisdiction over cases where any member of the plaintiff class is a citizen of a state different from any defendant, and where the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Here, the Plaintiffs' nationwide class includes all recipients of Defendant's Notice of Data Breach, which, upon information and belief, includes non-California citizens. Since Defendant is a California entity headquartered in California, there is minimal diversity between at least one member of the Plaintiffs' nationwide class and Defendant.

21. This Court also has subject matter jurisdiction over this case pursuant to 28. U.S.C. § 1331 because several of the claims for relief herein are dependent or predicted upon violating duties imposed upon Regal by federal law and regulation, including HIPAA, as more fully alleged below.

22. This Court has general personal jurisdiction over Defendant because Regal operates its principal place of business in California. Additionally, this Court also has specific personal jurisdiction over Defendant because it has minimum contacts with California, as it is located and conducts substantial business in or from California, and Plaintiffs' claims arise from Defendant's conduct in this State.

23. This Court has supplemental jurisdiction over any claims not arising, in whole or in part, from violation of federal law.

24. This Court is the proper venue for this action pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part of the events and omissions giving rise to Plaintiffs' claims occurred in this District, and because Defendant conducts a substantial part of its business within this District.

FACTUAL BACKGROUND

RMG's Obligation to Preserve and Protect Confidentiality and Privacy

25. Plaintiffs are informed and believe and thereupon allege that as a condition of service, Defendant required its patients – including Plaintiffs named herein – to provide

sensitive personal and private healthcare information, including the Private Information compromised in the Data Breach.

26. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' as a consequence of Private Information, Defendant assumed legal and equitable duties, and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

27. Given the highly sensitive nature of the PII and PHI it possessed and the sensitivity of the medical and health services it provides, RMG had a duty to safeguard, protect, and encrypt Plaintiffs' and Class Members' PII and PHI.

28. RMG's Notice Letter unequivocally acknowledges that it "understands the importance of safeguarding your personal information and takes that responsibility very seriously."

29. Defendant routinely provides each of its customers with a HIPAA compliant notice titled "NOTICE OF PRIVACY POLICY (the "Privacy Notice").[3]

30. The Privacy Notice, which is posted on Defendant's website, explains how it handles its patients' sensitive and confidential information and lists RMG's responsibilities to:

- maintain the privacy and security of your protected health information;
- let you know promptly if a breach occurs that may have compromised the privacy or security of your information;
- follow the duties and privacy practices described in this notice and give you a copy of it; and
- not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.[4]

[3] https://www.regalmed.com/Regal-en-us/assets/File/RMG-Notice-of-Privacy-Practice.pdf (last accessed Feb. 24, 2023).

[4] *Id.*

31. Defendant's Privacy Policy does not permit Defendant to disclose Plaintiffs' and Class Members' Private Information for any reason that would apply in this situation. The disclosure of Plaintiffs' and Class Members' Private Information via the Data Breach was not permitted per Defendant's own Privacy Policy.

32. Additionally, Defendant is duty bound to adhere to the HIPPA Compliance Policy relating to the Confidentiality of PHI. This policy clearly states:

> As required by state and HIPAA federal laws, Heritage Provider Network and its Affiliated Medical Groups will use reasonable care to assure confidentiality and privacy of personal information of patients, employees, and others, within the law, and protect against indiscriminate and unauthorized access to confidential medical or personal information.

33. Defendant's policy regarding the confidentiality of its information system network maintains that "[P]atient data accessible through the computer information system will be regarded confidential and will be available only to authorized users."

34. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information, and reasonably relied on Defendant's duty to keep such information confidential, securely maintained, solely used for business healthcare purposes, and only disclosed if expressly consented to by them, or authorized by law.

The December 1, 2022 Data Breach

35. On or about December 2, 2022, (and the right is reserved to drove it was sooner) Defendant noticed difficulty in accessing some of its servers. But even though it recognized that confidential and Private Information had been assessed and infiltrated, it was not until on or about February 1-2, 2023, and at various times thereafter, 60 or more days later, that Defendant began sending affected parties Notice Letters.[5]

[5] https://www.regalmed.com/notice2/ (last visited Feb. 24, 2023).

36. Notice posted on RMG's website disclosed that an investigation had determined that "malware was detected on some of our (RMG's) servers, which a threat actor utilized to access and exfiltrate data." Notice language made clear that the threat actor was an "unauthorized party," accessing and exfiltrating data" during a "ransomware cyberattack." The Private information included PII and PHI of Plaintiffs and Class Members, including, per Defendant's Notice, "name, social security number, date of birth, address, diagnosis and treatment, laboratory test results, prescription data, radiology reports, health plan member number, and phone number."

37. Plaintiffs and Class Members were advised by Regal's Notice Letter to take "take immediate steps to protect yourselves from potential harm" by, among other things, "monitor[ing] account statements, Explanation of Benefit forms, and credit bureau reports closely...[and] contact[ing] your state Consumer Protection Agency…[and] register[ing] a fraud alert with" the three major credit bureaus.

38. Defendant had obligations created by the Health Insurance Portability and Accountability Act ("HIPAA"), contract, industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and protect it from unauthorized access and disclosure.

39. Plaintiffs and Class Members had a reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep the Private Information they provided confidential and secure from unauthorized access and disclosure.

40. Defendant failed to use reasonable security procedures and practices appropriate to safeguard the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, consequently enabling and causing the exposure of Private Information of approximately 3,300,638 individuals.

41. Because of Defendant's negligence and misconduct in failing to keep their information confidential, the unencrypted Private Information of Plaintiffs and Class Members was "viewed or downloaded" and available for sale on the dark web, and exposed to falling into the hands of companies that will use the detailed Private Information for

targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can now access the PHI and PII of Plaintiffs and Class Members.

42. Plaintiffs and Class Members now face a real, present and substantially increased risk of fraud and identity theft and have lost the benefit of the bargain they made with Defendant when receiving medical or healthcare services.

Data Breaches Lead to Identity Theft and Cognizable Injuries.

43. The PII and PHI of consumers, such as Plaintiffs and Class Members, is valuable and has been commoditized in recent years.

44. Defendant was also aware of the significant repercussions that would result from its failure to do so and knew, or should have known, the importance of safeguarding the Private Information entrusted to it and of the foreseeable consequences if its data security were breached. Nonetheless, RMG failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

45. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen. As a result, victims suffer both immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

46. As a direct and proximate result of Defendant's conduct, Plaintiffs and the other Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. They must now be vigilant and continuously review their credit reports for suspected incidents of identity theft, educate themselves about security freezes, fraud alerts, and take steps to protect themselves against identity theft, which will extend indefinitely into the future.

47. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When such sensitive information is stolen, accounts become less secure, and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it

had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

48. Plaintiffs and the other Class Members also suffer ascertainable losses in the form of opportunity costs and the time and costs reasonably incurred to remedy or mitigate the effects of the Data Breach, including:

A. Monitoring compromised accounts for fraudulent charges;

B. Canceling and reissuing credit and debit cards linked to the financial information in possession of Defendant;

C. Purchasing credit monitoring and identity theft prevention;

D. Addressing their inability to withdraw funds linked to compromised accounts;

E. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

F. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

G. Placing freezes and alerts with credit reporting agencies;

H. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

I. Contacting their financial institutions and closing or modifying financial accounts;

J. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

K. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be cancelled; and,

L. Closely reviewing and monitoring financial accounts and credit reports for unauthorized activity for years to come.

49. Moreover, Plaintiffs and the other Class Members have an interest in ensuring that Defendant implement reasonable security measures and safeguards to maintain the integrity and confidentiality of the Private Information, including making sure that the storage of data or documents containing Private Information is not accessible by unauthorized persons, that access to such data is sufficiently protected, and that the Private Information remaining in the possession of Defendant is fully secure, remains secure, and is not subject to future theft.

50. As a further direct and proximate result of Defendant's actions and inactions, Plaintiffs and the other Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

51. As a direct and proximate result of Defendant's wrongful actions or omissions here, resulting in the Data Breach and the unauthorized release and disclosure of Plaintiffs' and other Class Members' Private Information, Plaintiffs and all Class Members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, inter alia, (i) the resulting increased and imminent risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; and (iii) emotional distress as a result of having their Private Information accessed and exfiltrated in the Data Breach.

RMG Was Well Aware of the Threat of Cyber Theft and Exfiltration in the Healthcare Industry

52. As a condition of its relationships with Plaintiffs and Class Members, Defendant required that Plaintiffs and Class Members entrust Defendant with highly sensitive and confidential PII and PHI and financial information. Defendant, in turn, stored that information on its system that was ultimately affected by the Data Breach.

53. Plaintiffs and Class Members were required to provide their PII and PHI and financial information to Defendant with the reasonable expectation and mutual

understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access and disclosure.

54. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and financial information. Plaintiffs and Class Members relied on Defendant to keep their PII and PHI and financial information confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

55. Defendant could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiffs' and Class Members' PII and PHI and financial information.

56. Defendant's overt negligence in safeguarding Plaintiffs' and Class Members' PII and PHI and financial information is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years. Further, as a healthcare provider, Defendant was on notice that companies in the healthcare industry are targets for data breaches.

57. The healthcare industry in particular has experienced a large number of high-profile cyberattacks. Cyberattacks, generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year, showing a 25% increase.[6] Additionally, according to the HIPAA Journal, the largest healthcare data breaches have been reported beginning in April 2021.[7]

58. This trend continues in 2022, and healthcare breaches continue to increase in record numbers.[8] Thus, Defendant was on further notice regarding the increased risks of inadequate cybersecurity. In February 2022, the cybersecurity arm of the U.S. Department

[6] 2020 Healthcare Data Breach Report, https://www.hipaajournal.com/2020-healthcare-databreach-report-us/ (last accessed Feb. 24, 2023).

[7] April 2021 Healthcare Data Breach Report, https://www.hipaajournal.com/april-2021- healthcare-data-breach-report/ (last accessed Feb. 24, 2023).

[8] June 2022 Healthcare Data Breach Report, https://www.hipaajournal.com/june-2022- healthcare-data-breach-report/ (last accessed Feb. 24, 2023).

of Health and Human Services ("HHS") issued a warning to hospitals and healthcare systems about a dramatic rise in cyberattacks, including ransomware attacks, urging facilities to shore up their cyber defenses.[9] Indeed, HHS's cybersecurity arm has issued yet another warning about increased cyberattacks that urged vigilance with respect to data security.[10]

59. In the context of data breaches, healthcare is "by far the most affected industry sector."[11] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[12]

60. A TENABLE study analyzing publicly disclosed healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in nearly 93% of the breaches."[13]

61. This is such a breach of cybersecurity where highly detailed PII and PHI records maintained, collected, and stored by a healthcare entity were accessed and/or acquired by a cybercriminal.

62. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately

---

[9] Rebecca Pifer, Tenet says 'cybersecurity incident' disrupted hospital operations, HEALTHCAREDIVE (Apr. 26, 2022), https://www.healthcaredive.com/news/tenet-sayscybersecurity-incident-disrupted-hospital-operations/622692/ (last accessed Feb. 24, 2023).

[10] Id. (HHS warned healthcare providers about the increased potential for attacks by a ransomware group called Hive, "[c]alling it one of the 'most active ransomware operators in the cybercriminal ecosystem,' the agency said reports have linked Hive to attacks on 355 companies within 100 days of its launch last June — nearly three a day.").

[11] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid19-era-breaches (last accessed Feb. 24, 2023).

[12] *See id.*

[13] Tenable Security Response Team, *Healthcare Security,* TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid19-era-breaches (last accessed Feb. 24, 2023).

performed the duty of preparing for such an imminent attack. This is especially true given that Defendant is a large, sophisticated operation with the resources to put adequate data security protocols in place.

63. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Plaintiffs' and Class Members' PII and PHI and financial information from being compromised.

Defendant Had an Obligation to Protect the PII and PHI

64. Defendant has a statutory duty under HIPAA and other federal or state statutes to safeguard Plaintiffs' and Class Members' data.

65. Moreover, Plaintiffs and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data, independent of any statute.

Defendant's Conduct Violates Federal Law, Including the Rules and Regulations of HIPAA and HITECH

66. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

67. Defendant is a covered entity pursuant to HIPAA. See 45 C.F.R. § 160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. See 45 C.F.R. Part 160 and Part 164, Subparts A through E.

68. Defendant is a covered entity pursuant to the Health Information Technology Act ("HITECH").[14] See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

69. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

70. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

71. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

72. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

73. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

74. HIPAA's Security Rule requires Defendant to do the following:

a) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c) Protect Against reasonably anticipated uses or disclosures of such information that are not permitted; and

[14] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

d) Ensure compliance by its workforce.

75. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

76. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

77. Plaintiffs' and Class Members' Personal and Medical Information, including their PII and PHI, is "protected health information" as defined by 45 CFR § 160.103.

78. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

79. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

80. Plaintiffs' and Class Members' personal and medical information, including their PII and PHI, is "unsecured protected health information" as defined by 45 CFR § 164.402.

81. Plaintiffs' and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

82. Plaintiffs' and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E

as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

83. Plaintiffs' and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

84. Plaintiffs' and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

85. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

86. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

87. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

88. This Data Breach is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

89. The Data Breach could have been prevented if Defendant implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

90. It can be inferred from Defendant's Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Representative Plaintiffs' and Class Members' PII and PHI.

91. Upon information and belief, Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system and safeguards to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data, including identifying internal and external risks of a security breach;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*; and

k. Retaining information past a recognized purpose and not deleting it.

92. Upon information and belief, prior to the Breach, Defendant was aware of its security failures but failed to correct them or to disclose them to the public, including Plaintiffs and Class Members.

93. The implementation of proper encryption, logging, detection, training, and monitoring protocols requires affirmative acts. Accordingly, Defendant knew or should have known that it did not make such actions and failed to implement adequate data security practices.

94. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

95. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the PII and PHI of Plaintiffs and Class Members; and without the supervision of the Court via injunctive relief, Representative Plaintiffs' and Class Members' PII and PHI remains at risk of subsequent Data Breaches.

96. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining,

securing, safeguarding, deleting, and protecting the PII and PHI and financial information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII and PHI and financial information of Plaintiffs and Class Members.

97. Defendant owed a duty to Plaintiffs and Class Members to design, maintain, and test its computer systems, servers and networks to ensure that the PII and PHI and financial information in its possession was adequately secured and protected.

98. Defendant owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII and PHI and financial information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

99. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would immediately detect a breach on its data security systems in a timely manner.

100. Defendant owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

101. Defendant owed a duty to Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII and PHI and/or financial information from theft because such an inadequacy would be a material fact in the decision to entrust this PII and PHI and/or financial information to Defendant.

102. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

103. Defendant owed a duty to Plaintiffs and Class Members to encrypt and/or more reliably encrypt Plaintiffs' and Class Members' PII and PHI and financial information and monitor user behavior and activity in order to identity possible threats.

104. Defendant owed a duty to Plaintiffs and Class Members to mitigate the harm suffered by the Representative Plaintiffs' and Class Members' as a result of the Data Breach.

Defendant Violated FTC Guidelines Prohibiting Unfair or Deceptive Acts

105. RMG is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See e.g., FTC v. Wyndham Corp.*, 799 F.3d 236 (3d Cir. 2015).

106. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[15]

107. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[16]

108. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

[15] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Feb. 24, 2023).

[16] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Feb. 24, 2023).

109. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

110. RMG failed to properly implement basic data security practices. RMG's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

111. RMG was at all times fully aware of its obligations to protect Plaintiffs' and Class Members' Private Information because of its business model of collecting Private Information and storing such information. RMG was also aware of the significant repercussions that would result from its failure to do so.

Value of the Relevant Sensitive Information

112. While the greater efficiency of electronic health records translates to cost savings for providers, it also comes with the risk of privacy breaches. These electronic health records contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, RX's, treatment plans) that is valuable to cyber criminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PII and PHI and financial information are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on a number of underground internet websites. Unsurprisingly, the healthcare industry is at high risk for and acutely affected by cyberattacks.

113. The high value of PII and PHI and financial information to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold

at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[17] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[18] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[19]

114. Between 2005 and 2019, at least 249 million people were affected by health care data breaches.[20] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[21] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03% of overall health data breaches, according to cybersecurity firm Tenable.[22]

115. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Plaintiffs and Class Members for the rest of their lives. They will need to remain constantly vigilant.

116. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes

---

[17] Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-darkweb-how-much-it-costs/ (last accessed Feb. 24, 2023).

[18] Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-darkweb-how-much-it-costs/ (last accessed Feb. 24, 2023).

[19] In the Dark, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Feb. 24, 2023).

[20] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133 (last accessed Feb. 24, 2023).

[21] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed Feb. 24, 2023).

[22] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches (last accessed Feb. 24, 2023).

"identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

117. Identity thieves can use PII and PHI and financial information, such as that of Representative Plaintiffs and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

118. The ramifications of Defendant's failure to keep secure Plaintiffs' and Class Members' PII and PHI and financial information are long lasting and severe. Once PII and PHI and financial information is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PII and PHI and/or financial information of Plaintiffs and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII and PHI and/or financial information for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

119. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and PHI and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that

> attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[23]

120. The harm to Plaintiffs and Class Members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical- related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[24]

121. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[25]

122. If cyber criminals manage to access financial information, health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Plaintiffs and Class Members.

123. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[26] Almost half of medical identity theft victims lose their healthcare coverage as

---

[23] 47 Report to Congressional Requesters, GAO, at 29 (June 2007), available at: http://www.gao.gov/new.items/d07737.pdf (last accessed Feb. 24, 2023).

[24] Michael Ollove, The Rise of Medical Identity Theft in Healthcare, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/ (last accessed Feb. 24, 2023).

[25] *Id.*

[26] See Elinor Mills, Study: Medical Identity Theft is Costly for Victims, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed Feb. 24, 2023).

a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[27]

124. Data breaches are preventable.[28] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[29] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised."[30]

125. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[31]

126. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards and concomitant duties mandated and required by HIPAA regulations.

Defendant's Delayed Response to the Breach

127. Time is of the essence when highly sensitive PII and PHI is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII and PHI of Plaintiffs and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiffs and Class Members are now subject to the present and continuing risk of fraud,

---

[27] Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, available at https://www.experian.com/blogs/ask-experian/healthcare-data-breachwhat-to-know-about-them-and-what-to-do-after-one/ (last accessed Feb. 24, 2023).

[28] Lucy L. Thompson, Despite the Alarming Trends, Data Breaches Are Preventable, in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)

[29] *Id*. at 17.

[30] *Id*. at 28.

[31] *Id.*

identity theft, and misuse resulting from the possible publication of their PII and PHI, especially their Social Security numbers and sensitive medical information, onto the Dark Web. Plaintiffs and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing hundreds of thousands of Social Security numbers and/or specific, sensitive medical information.

128. Despite this understanding, Defendant did not begin informing affected individuals, including Plaintiffs and Class Members, about the Data Breach for 60 days and longer. The Notice Letter provided only scant details of the Data Breach and Defendant's recommended next steps.

129. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[32]

130. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[33] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[34] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating

[32] U.S. BUREAU OF LABOR STATISTICS, Wage Worker Survey, available at https://www.bls.gov/opub/reports/minimumwage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%2 0%247.25%20per%20hour (last visited Feb. 24, 2023); see also U.S. BUREAU OF LABOR STATISTICS, Employment And Average Hourly Earnings By Industry, available at https://www.bls.gov/charts/employment-situation/employment-and-average-hourly-earnings-byindustry-bubble.htm (last visited Feb. 24, 2023) (finding that on average, private-sector workers make $1,312.80 per 40-hour work week.).

[33] See https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-jameswallman.html (last visited Feb. 24, 2023).

[34] *Id.*

with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

131. Plaintiffs and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek remuneration for the loss of valuable time as another element of damages.

I. CLASS ALLEGATIONS

132. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiffs assert common law and statutory claims, as more fully alleged hereinafter, on behalf of the following Nationwide Class and California Class, defined as follows:

> **Nationwide Class**: All residents of the United States whose PII or PHI was accessed or otherwise compromised as a result of the Regal Medical Group, Inc. Data Breach.
>
> **California Class:** All residents of the state of California whose PII or PHI was accessed or otherwise compromised as a result of the Regal Medical Group, Inc. Data Breach.

Members of the Nationwide Class and the California Class are referred to herein collectively as "Class Members" or "Class."

133. Excluded from the Class are Defendant, any entity in which Defendant have a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

134. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

135. **Numerosity**: The exact number of members of the Class is unknown to Plaintiffs at this time but Regal operates numerous medical centers. Regal acknowledges that the number of "individuals affected" by the Regal Data Breach was over 3 million persons, indicating that there are more than 3 million members of the Class, making joinder

of each individual impracticable. Ultimately, members of the Class will be readily identified through Defendant's records.

136. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a) Whether Defendant failed to adequately safeguard Plaintiffs' and the Class Members' PII and PHI;

b) Whether Defendant failed to protect Plaintiffs' and the Class Members' PII and PHI, as promised;

c) Whether Defendant's computer system systems and data security practices used to protect Plaintiffs' and the Class Members' PII and PHI violated HIPAA, federal, state and local laws, or Defendant's duties;

d) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and the Class Members' PII and PHI properly and/or as promised;

e) Whether Defendant violated the consumer protection statutes, data breach notification statutes, state unfair practice statutes, state privacy statutes, and state medical privacy statutes, HIPAA, and/or FTC law or regulations, imposing duties upon Regal, applicable to Plaintiffs and Class Members;

f) Whether Defendant failed to notify Plaintiffs and members of the Class about the Regal Data Breach as soon as practical and without delay after the Regal Data Breach was discovered;

g) Whether Defendant acted negligently in failing to safeguard Plaintiffs' and the Class Members' PII and PHI;

h) Whether Defendant entered into contracts with Plaintiffs and the Class Members that included contract terms requiring Defendant to protect the

confidentiality of Plaintiffs' PII and PHI and have reasonable security measures;

i) Whether Defendant's conduct described herein constitutes a breach of their contracts with Plaintiffs and each of the Class Members;

j) Whether Defendant should retain the money paid by Plaintiffs and each of the Class Members to protect their PII and PHI;

k) Whether Plaintiffs and the Class Members are entitled to damages as a result of Defendant's wrongful conduct;

l) Whether Plaintiffs and the Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

m) What equitable relief is appropriate to redress Defendant's wrongful conduct; and

n) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Class Members.

137. **Typicality**: Plaintiffs' claims are typical of the claims of each of the Class Members. Plaintiffs and the Class Members sustained damages as a result of Defendant's uniform wrongful conduct during transactions with them.

138. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex litigation and class actions. Plaintiffs have no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiffs. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class, and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Class.

139. **Separateness**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Class. Furthermore, the Regal database still exists, and is still

vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the Regal database.

140. **Class-wide Applicability**: This case is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Plaintiffs and proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class, and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant's practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiffs' challenge to those practices hinges on Defendant's conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiffs.

141. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if Class Members could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

142. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations by reference.

143. Plaintiffs and Class Members were required to submit PII and PHI to healthcare providers, including Defendant, in order to obtain insurance coverage and/or to receive healthcare services.

144. Defendant knew, or should have known, of the risks and responsibilities inherent in collecting and storing the PII and PHI of Plaintiffs and Class Members.

145. As described above, Defendant owed a duty of care to Plaintiffs and Class Members whose PII and PHI had been entrusted to Defendant.

146. Defendant breached its duty to Plaintiffs and Class Members by failing to secure their PII and PHI from unauthorized disclosure to third parties.

147. Defendant acted with wanton disregard for the security of Plaintiffs and Class Members' PII and PHI.

148. A "special relationship" exists between Defendant and the Plaintiffs and Class Members. Defendant entered into a "special relationship" with Plaintiffs and Class Members because it collected and/or stored the PII and PHI of Plaintiffs and the Class Members.

149. But for Defendant's wrongful and negligent breach of its duty owed to Plaintiffs and the Class Members, Plaintiffs and the Class Members would not have been injured.

150. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duty. Defendant knew or should have known it was failing to meet its duty, and that Defendant's breach of such duties would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the unauthorized exposure of their PII and PHI.

151. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

152. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations by reference.

153. Pursuant to HIPAA (42 U.S.C. §1302d *et. seq*.), Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' PII and PHI.

154. Defendant breached its duty to Plaintiffs and Class Members under HIPAA (42 U.S.C. § 1302d *et. seq.*), by failing to implement reasonable safeguards to protect Plaintiffs' and Class Members' PII and PHI from unauthorized access.

155. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

156. But for Defendant's wrongful and negligent breach of its duty owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

157. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duty, and that Defendant's breach of that duty would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the unauthorized access to their PII and PHI.

158. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III

Breach of Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiffs and the Class)

159. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations by reference.

160. Plaintiffs and Class Members entered into valid, binding, and enforceable express or implied contracts with Defendant, as alleged above.

161. The contracts respecting which Plaintiffs and Class Members were intended beneficiaries were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Defendant would act fairly and in good faith in carrying out its contractual obligations to take reasonable measures to protect Plaintiffs' PII and PHI from unauthorized disclosure and to comply with state laws and regulations.

162. A "special relationship" exists between Defendant and the Plaintiffs and Class Members. Defendant entered into a "special relationship" with Plaintiffs and Class Members who sought medical services or treatment at Regal affiliated facilities and, in doing so, entrusted Defendant, pursuant to its requirements and Privacy Notice, with their PII and PHI.

163. Despite this special relationship with Plaintiffs, Defendant did not act in good faith and with fair dealing to protect Plaintiffs' and Class Members' PII and PHI.

164. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Defendant.

165. Defendant's failure to act in good faith in complying with the contracts denied Plaintiffs and Class Members the full benefit of their bargain, and instead they received healthcare and related services that were less valuable than what they paid for and less valuable than their reasonable expectations.

166. Accordingly, Plaintiffs and Class Members have been injured as a result of Defendant's breach of the covenant of good faith and fair dealing and are entitled to damages and/or restitution in an amount to be proven at trial.

///

///

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

167. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations as if fully set forth herein.

168. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardian of Plaintiffs and Class Members' PII and PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII and PHI, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs and Class Members' PII and PHI; (2) to timely notify Plaintiffs and Class Members of an unauthorized disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and do store.

169. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with its patients, in particular, to keep secure their PII and PHI from disclosure without authorization from Plaintiffs and the Class Members.

170. Defendant breached its fiduciary duty owed to Plaintiffs and Class Members by failing to notify and/or warn Plaintiffs and Class Members of the unauthorized disclosure of their PII and PHI.

171. Defendant breached its fiduciary duty to Plaintiffs and Class Members by failing to safeguard Plaintiffs' and Class Members' PII and PHI from unauthorized disclosure.

172. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the compromise of their PII and PHI; and (ii) the diminished value of the services they received.

173. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
Breach of Duty
(On behalf of Plaintiffs and the Class)

174. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations by reference.

175. Defendant accepted the special confidence placed in its by Plaintiffs and Class Members. There was an understanding between the parties that the healthcare service provider Defendant would act for the benefit of Plaintiffs and Class Members in preserving the confidentiality of their PII and PHI.

176. Defendant became the guardian of Plaintiffs' and Class Members' PII and PHI and accepted a fiduciary duty to act primarily for the benefit of its patients, including Plaintiffs and the Class Members, including safeguarding Plaintiffs' and the Class Members' PII and PHI.

177. Defendant's fiduciary duty to act for the benefit of Plaintiffs and Class Members pertains as well to matters within the scope of Defendant's medical relationship with its patients, in particular, to keep secure the PII and PHI of those patients.

178. Defendant breached its fiduciary duty to Plaintiffs and Class Members by (a) failing to protect their PII and PHI to Plaintiffs and the Class; (b) by failing to notify Plaintiffs and the Class Members of the unauthorized disclosure of the PII and PHI; and (c) by otherwise failing to safeguard Plaintiffs' and the Class Members' PII and PHI.

179. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiffs and/or Class Members have suffered and/or will suffer injury, including but not limited to: (a) the compromise of their PII and PHI; and (b) the diminished value of the services they received as a result of unauthorized exposing of Plaintiffs' and Class Members' PII and PHI.

180. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VI
Breach of Implied Contract
(On behalf of Plaintiffs and the Class)

181. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations by reference.

182. Defendant required Plaintiffs and the Class Members to provide and entrust their PII and PHI and financial information as a condition of obtaining medical care and medical devices from Defendant.

183. Plaintiffs and the Class Members paid money to Defendant in exchange for goods and services, as well as Defendant's promises to protect their protected health information and other PII from unauthorized disclosure.

184. Defendant promised to comply with HIPAA and HITECH standards and to make sure that Plaintiffs' and Class Members' protected health information and other PII would remain protected.

185. Through its course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' PII and PHI and financial information.

186. Defendant required Plaintiffs and Class Members to provide and entrust their PII and PHI and financial information, including medical information, record or account numbers, names, Social Security numbers, Driver's License numbers, email addresses, and dates of birth.

187. Defendant solicited and invited Plaintiffs and Class Members to provide their PII and PHI and financial information as part of Defendant's regular business practices.

Plaintiffs and Class Members accepted Defendant's offers and provided their PII and PHI and financial information to Defendant.

188. As a condition of being direct customers/patients of Defendant, Plaintiffs and Class Members provided and entrusted their PII and PHI and financial information to Defendant. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if its data had been breached and compromised or stolen.

189. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide its PII and PHI and financial information to Defendant, in exchange for, amongst other things, the protection of its PII and PHI and financial information. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

190. Plaintiffs and the Class Members would not have entrusted their PII and PHI to Defendant in the absence of Defendant's implied promise to adequately safeguard this confidential personal and medical information.

191. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

192. Defendant breached the implied contracts it made with Plaintiffs and the Class by making their PII and PHI accessible from the internet (regardless of any mistaken belief that the information was protected) and failing to make reasonable efforts to use the latest security technologies designed to help ensure that the PII and PHI was secure, failing to encrypt Plaintiffs' and Class Members' sensitive PII and PHI, failing to safeguard and protect their medical, personal and financial information and by failing to provide timely and accurate notice to them that medical, personal and financial information was compromised as a result of the data breach.

193. Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their PII and PHI and financial information and by failing to provide timely and accurate notice to them that their PII and PHI and financial information was compromised as a result of the Data Breach.

194. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to comply with its promise to abide by HIPAA and HITECH.

195. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

196. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

197. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

198. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

199. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

200. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of

electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

201. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations in violation of 45 CFR 164.306(a)(94).

202. Defendant further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*

203. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

204. Defendant further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PII and PHI.

205. Defendant's failures to meet these promises constitute breaches of the implied contracts.

206. Because Defendant allowed unauthorized access to Plaintiffs' and Class Members' PII and PHI and failed to safeguard the PII and PHI, Defendant breached its contracts with Plaintiffs and Class Members.

207. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

208. As a result of Defendant's breach of implied contract, Plaintiffs and the Class Members are entitled to and demand actual, consequential, and nominal damages.

COUNT VII
Violation of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq.*
(On Behalf of Plaintiffs and the Class)

209. Plaintiffs, on behalf of the Class, restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

210. Defendant is "a provider of health care," as defined in Cal. Civ. Code §56.05(m), and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

211. At all relevant times, Defendant was a health care provider because they had the "purpose of maintaining medical information to make the information available to the individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manager his or her information, or for the diagnosis or treatment of the individual."

212. As a provider of health care or a contractor, Defendant is required by the CMIA to ensure that medical information regarding patients is not disclosed or disseminated and/or released without patient's authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, 56.36, and 56.101.

213. As a provider of health care or a contractor, Defendant is required by the CMIA not to disclose medical information regarding a patient without first obtaining an authorization under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, and 56.104.

214. Defendant is a person/entity licensed under California under California's Business and Professions Code, Division 2. See Cal. Bus. Prof. Code § 4000, *et seq.*

215. Plaintiffs and Class Members are "patients" as defined in CMIA, Cal. Civ. Code §56.05(k) ("'Patient' means any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains").

216. Furthermore, Plaintiffs and Class Members, as patients and customers of Defendant, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant's computer network, and were patients on or before the date of the Data Breach.

217. Defendant disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the affirmative actions of Defendant's employees, which allowed the hackers to see and obtain Plaintiffs' and Class Members' medical information.

218. Defendant negligently created, maintained, preserved, stored, and then exposed Plaintiffs' and Class Members' individually identifiable "medical information," within the meaning of Cal. Civ. Code § 56.05(j), including Plaintiffs' and Class members' names, addresses, medical information, and health insurance information, that alone or in combination with other publicly available information, reveals their identities. Specifically, Defendant knowingly allowed and affirmatively acted in a manner that allowed unauthorized parties to access, exfiltrate, and actually view Plaintiffs' and Class Members' confidential Private Information.

219. Defendant's negligence resulted in the release of individually identifiable medical information pertaining to Plaintiffs and Class Members to unauthorized persons and the breach of the confidentiality of that information. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiffs' and Class Members' medical information in a manner that preserved the confidentiality of the information contained therein, in violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

220. Defendant also violated Sections 56.06 and 56.101 of the CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction, or disposal of confidential personal medical information.

221. Plaintiffs' and Class Members' medical information was accessed and actually viewed by hackers in the Data Breach.

222. Plaintiffs' and Class Members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

223. Defendant's computer systems did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A). As a direct and proximate result of Defendant's above-noted wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiffs and the Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia:

a. present, imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud –risks justifying expenditures for protective and remedial services for which they are entitled to compensation;

b. invasion of privacy;

c. breach of the confidentiality of the PHI;

d. statutory damages under the California CMIA;

e. deprivation of the value of their PHI, for which there is well-established national and international markets; and/or,

f. the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

224. As a direct and proximate result of Defendant's wrongful actions, inaction, omission, and want of ordinary care that directly and proximately caused the release of Plaintiffs' and Class Members' Private Information, Plaintiffs' and Class Members'

personal medical information was viewed by, released to, and disclosed to third parties without Plaintiffs' and Class Members' written authorization.

225. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiffs' and Class Members' medical information in a manner that preserved the confidentiality of the information contained therein violated the CMIA.

226. Plaintiffs and the Class Members were injured and have suffered damages, as described above, from Defendant's illegal and unauthorized disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, which allows for actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorneys' fees, expenses and costs.

COUNT VIII
Invasion of Privacy
Cal. Const. Art. 1 § 1
(On Behalf of Plaintiffs and the Class)

227. Plaintiffs, on behalf of the Class, restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

228. Plaintiffs bring this Count on their own behalf and on behalf of themselves and the Class.

229. California established the right to privacy in Article I, Section 1 of the California Constitution.

230. Plaintiffs and the Class had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

231. Defendant, headquartered in California and offering its healthcare services from California, owed a duty to its current and former patients, including Plaintiffs and the Class, to keep their Private Information contained as a part thereof, confidential.

232. Defendant failed to protect and released to unknown and unauthorized third parties the PII and PHI of Plaintiffs and the Class Members.

233. Defendant enabled and allowed unauthorized and unknown third parties access to and examination of the Private Information of Plaintiffs and the Class Members, by way of Defendant's failure to protect the PII and PHI.

234. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiffs and the Class Members is highly offensive to a reasonable person.

235. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Class Members disclosed their Private Information to Defendant as part of their medical care or employment with Defendant, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure.

236. Plaintiffs and the Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

237. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

238. Defendant acted with a knowing state of mind when they permitted the Data Breach to occur because they were with actual knowledge that its information security practices were inadequate and insufficient.

239. Because Defendant acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Class Members.

240. As a proximate result of the above acts and omissions of Defendant, the Private Information of Plaintiffs and the Class Members was disclosed to third parties without authorization, causing Plaintiffs and the Class to suffer damages.

241. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class Members in that the PII and PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

COUNT IX
California Unfair Competition Law
Cal. Bus. & Prof. Code, § 17200, *et seq.*
(On Behalf of Plaintiffs and the Class)

242. Plaintiffs, on behalf of the Class, incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

243. Defendant is both organized under the laws of California and headquartered in California. Defendant violated California's Unfair Competition Law ("UCL") (Cal. Bus. & Prof. Code, § 17200, *et seq.*) by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

a. by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard their PII and PHI from unauthorized disclosure, release, data breach, and theft; representing and advertising that they did and would comply with the requirement of relevant federal and state laws pertaining to the privacy and security of the Class' PII and PHI; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class' PII and PHI;

b. by soliciting and collecting Class members' PII and PHI with knowledge that the information would not be adequately protected; and by storing

Plaintiffs' and Class Members' PII and PHI in an unsecure electronic environment;

c. by failing to disclose the Data Breach in a timely and accurate manner, in violation of California Civil Code section 1798.82;

d. by violating the privacy and security requirements of HIPAA, 42 U.S.C. §1302d, *et seq.;*

e. by violating the CMIA, California Civil Code section 56, *et seq.*; and

f. by violating the CCRA, California Civil Code section 1798.82.

244. These unfair acts and practices were immortal, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and Class Members. Defendant's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq.*, CMIA, Cal. Civ. Code, § 56, *et seq.*, and the CCRA, Cal. Civ. Code, § 1798.81.5.

245. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiffs and the Class Members were injured and lost money or property, including but not limited to the overpayments Defendant received to take reasonable and adequate security measures (but did not), the loss of their legally protected interest in the confidentiality and privacy of their PII and PHI, and additional losses described above.

246. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and PHI and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

247. Plaintiffs seek relief under the UCL, including restitution to the Class of money or property that the Defendant may have acquired by means of Defendant's deceptive,

unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. Proc., § 1021.5), and injunctive or other equitable relief.

COUNT X
California Consumer Records Act
Cal. Civ. Code § 1798.82, *et seq.*
(On Behalf of Plaintiffs and the Class)

248. Plaintiffs, on behalf of the Class, incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

249. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay . . . ."

250. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code, § 1798.82(b)).

251. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

i. The name and contact information of the reporting person or business subject to this section;

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

252. If the information is possible to determine at the time the notice is provided, then any of the following:

1. The date of the breach;
2. The estimated date of the breach; or
3. The date range within which the breach occurred. The notification shall also include the date of the notice.

c. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

d. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

e. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

253. The Data Breach described herein constituted a "breach of the security system" of Defendant.

254. As alleged above, Defendant unreasonably delayed informing Plaintiffs and Class Members about the Data Breach, affecting their PII and PHI, after Defendant knew the Data Breach had occurred.

255. Defendant failed to disclose to Plaintiffs and the Class Members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PII and PHI when Defendant knew or reasonably believed such information had been compromised.

256. Defendant's ongoing business interests gave Defendant incentive to conceal the Data Breach from the public to ensure continued revenue.

257. Upon information and belief, no law enforcement agency instructed Defendant that timely notification to Plaintiffs and the Class Members would impede its investigation.

258. As a result of Defendant's violation of California Civil Code section 1798.82, Plaintiffs and the Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiffs and Class members because their stolen information would have had less value to identity thieves.

259. As a result of Defendant's violation of California Civil Code section 1798.82, Plaintiffs and the Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

260. Plaintiffs and the Class Members seek all remedies available under California Civil Code section 1798.84, including, but not limited to the damages suffered by Plaintiffs and the other Class Members, including but not limited to benefit-of-the-bargain and time spent monitoring their accounts for identity theft and medical identity theft, and equitable relief.

261. Defendant's misconduct as alleged herein is fraud under California Civil Code section 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendant conducted with the intent on the part of Defendant of depriving Plaintiffs and the Class Members of "legal rights or otherwise causing injury." In addition, Defendant's misconduct as alleged herein is malice or oppression under California Civil Code section 3294(c)(1) and (c) in that it was despicable conduct carried on by Defendant with a willful and conscious disregard of the rights or safety of Plaintiffs and the Class Members and despicable conduct that has subjected Plaintiffs and the Class Members to crewel and unjust hardship in conscious disregard of their rights. As a result, Plaintiffs and the Class Members are entitled to punitive damages against Defendant under California Civil Code section 3294(a).

COUNT XI
California Confidentiality of Medical Information Act,
Cal. Civ. Code § 56, *et seq.*
(On Behalf of Plaintiffs and the Class)

262. Plaintiffs, on behalf of the Class, incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

263. Defendant is a "contractor," as defined in California Civil Code section 56.05(d), and "a provider of health care," as defined in California Civil Code section 56.06, and is therefore subject to the requirements of the CMIA, California Civil Code sections 56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

264. Defendant is a person licensed under California under California's Business and Professions Code, Division 2. (*See*, Cal. Bus. Prof. Code, § 4000, *et seq.*) Regal therefore qualifies as a "provider of health care," under the CMIA.

265. Plaintiffs and the Class Members are "patients," as defined in CMIA, California Civil Code section 56.05(k) ("'Patient' means any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains.").

266. Defendant disclosed "medical information," as defined in CMIA, California Civil Code section 56.05(j), to unauthorized persons without first obtaining consent, in violation of California Civil Code section 56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the affirmative actions of Regal's employees, which allowed the hackers to see and obtain Plaintiffs' and the Class Members' medical information.

267. Defendant's negligence resulted in the release of individually- identifiable medical information pertaining to Plaintiffs and the Class Members to unauthorized persons and the breach of the confidentiality of that information. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiffs' and Class Members' medical information in a manner that preserved the confidentiality of the

information contained therein, in violation of California Civil Code sections 56.06 and 56.101(a).

268. Defendant's computer systems did not protect and preserve the integrity of electronic medical information in violation of California Civil Code section 6.101(b)(1)(A).

269. Plaintiffs and the Class Members were injured and have suffered damages, as described above, from Defendant's negligent release of their medical information in violation of California Civil Code sections 56.10 and 56.101, and therefore seek relief under Civil Code sections 56.35 and 56.36, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorney fees, expenses and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class, prays for relief and judgment against Defendant as follows:

A. certifying the Class pursuant to Section 382 of the Code of Civil Procedure, appointing Plaintiffs as representatives of the Class, and designating Plaintiffs' counsel as Class Counsel;

B. declaring that Defendant's conduct violates the laws referenced herein;

C. finding in favor of Plaintiffs and the Class on all counts asserted herein;

D. awarding Plaintiffs and the Class compensatory damages and actual damages, trebled, in an amount exceeding $5,000,000, to be determined by proof;

E. awarding Plaintiffs and the Class appropriate relief, including actual, nominal and statutory damages;

F. awarding Plaintiffs and the Class punitive damages;

G. awarding Plaintiffs and the Class civil penalties;

H. granting Plaintiffs and the Class declaratory and equitable relief, including restitution and disgorgement;

I. enjoining Defendant from continuing to engage in the wrongful acts and

practices alleged herein;

J. awarding Plaintiffs and the Class the costs of prosecuting this action, including expert witness fees;

K. awarding Plaintiffs and the Class reasonable attorneys' fees and costs as allowable by law;

L. awarding pre-judgment and post-judgment interest; and

M. granting any other relief as this Court may deem just and proper.

II. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: February 28, 2023

Respectfully submitted,

BARRACK, RODOS & BACINE

By: */s/ STEPHEN R. BASSER*
STEPHEN R. BASSER, State Bar No. 121590
SAMUEL M. WARD, State Bar No. 216562
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874
sbasser@barrack.com

POMERANTZ LLP
JORDAN L. LURIE, State Bar No. 130013
ARI Y. BASSER, State Bar No. 272618
1100 Glendon Avenue, 15th Floor
Los Angeles, CA 90024
Telephone: (310) 432-8492
abasser@pomlaw.com
jllurie@pomlaw.com

EMERSON FIRM, PLLC
JOHN G. EMERSON*
2500 Wilcrest, Suite 300
Houston, TX 77042
Telephone: (800) 551-8649
Facsimile: (501) 286-4659
jemerson@emersonfirm.com

Counsel for Plaintiffs

**Pro Hac Vice* application to be filed